Per i computer è alle porte una nuova rivoluzione, che li renderà molto più veloci: quella "quantistica"

Dai bit ai qubit

I prototipi sono stati costruiti. E il primo modello commerciale è stato annunciato per il 2008.

Secondo un gruppo sempre più folto di scienziati, il futuro dell'informatica non ha nulla a che vedere con i "vecchi" microchip fatti di miliardi e miliardi di "semplici" transistor di silicio. Piuttosto sarà popolato da nuove macchine raffinatissime costituite da molecole, raggi laser e superconduttori; che funzionano non secondo le leggi "classiche" dell'elettronica, ma secondo quelle bizzarre della "meccanica quantistica". Un mondo strano, in cui le particelle possono trovarsi contemporaneamente in posti diversi e possono sincronizzarsi tra loro come se fossero un tutt'uno (*v. Focus n° 122*). Per dar vita a macchine sorprendenti, capaci di svolgere in un istante più calcoli di quelli che tutti i computer attuali svolgerebbero nel corso dell'intera vita dell'universo.

Pura fantascienza? Niente affatto: i primissimi computer quantistici ci sono già e le applicazioni commerciali sono state annunciate per il 2008.

Dono di ubiquità

Per capire bene in che cosa consistono, bisogna innanzitutto ricordare come funziona un computer "classico": «L'informatica tradizionale si basa su sequenze di 0 e 1 (i bit) elaborate per mez-

I MIRACOLI DELLA QUANTISTICA 1) Come una moneta inclinata

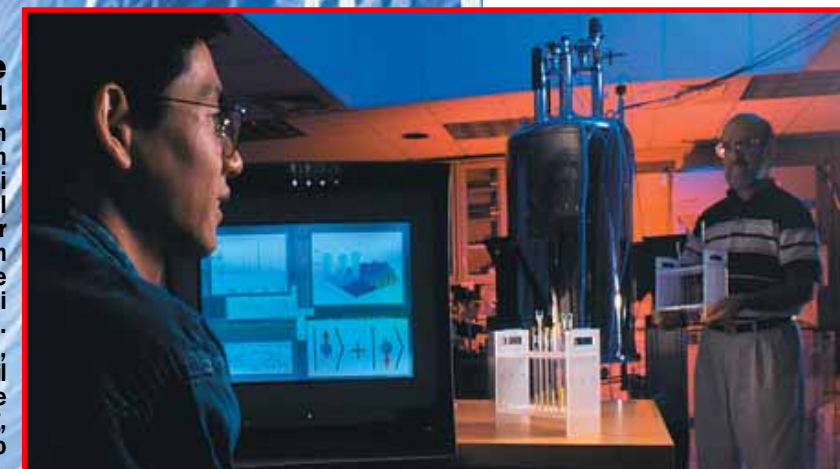
I computer classici si basano sui bit, sequenze di 0 e 1 capaci di codificare qualsiasi numero e qualsiasi lettera dell'alfabeto. I computer quantistici, invece, elaborano i "bit quantistici", o "qubit". In casi particolari, i qubit valgono 0 o 1, come i bit. Ma, in generale, i qubit possono assumere anche valori "intermedi" e immagazzinare, così, una maggiore quantità di informazione.

Un BIT tradizionale, come quelli usati dai computer normali, può valere 0 o 1, l'equivalente di testa o croce al lancio di una moneta.

Un QUBIT può essere invece in una "sovrapposizione" di 0 e 1. Se si legge l'informazione, però, il risultato può essere solo 0 o 1 (come per i computer classici). Il qubit si può rappresentare come una moneta inclinata. L'angolo d'inclinazione permette di calcolare la probabilità che la misura del qubit dia come risultato 0 oppure 1.

Aggiungere più qubit è come aggiungere monete, ciascuna con la sua inclinazione. Già con pochi qubit, si possono fare calcoli molto complessi.

Il primo è del 2001

Laboratorio Ibm ad Almaden (Stati Uniti). Qui è stato creato il primo computer quantistico, in grado di svolgere semplici calcoli matematici. In primo piano, sulla sinistra, il ricercatore Isaac Chuang, che ha coordinato la ricerca.

2) Dov'è l'asso di picche?

Un giocatore che guarda le sue carte secondo le regole dei computer classici (**1**) le esamina tutte una a una.
Un giocatore che usa le regole dei computer quantistici (**2**), invece, può esaminarle tutte contemporaneamente in un colpo solo: è molto più veloce.

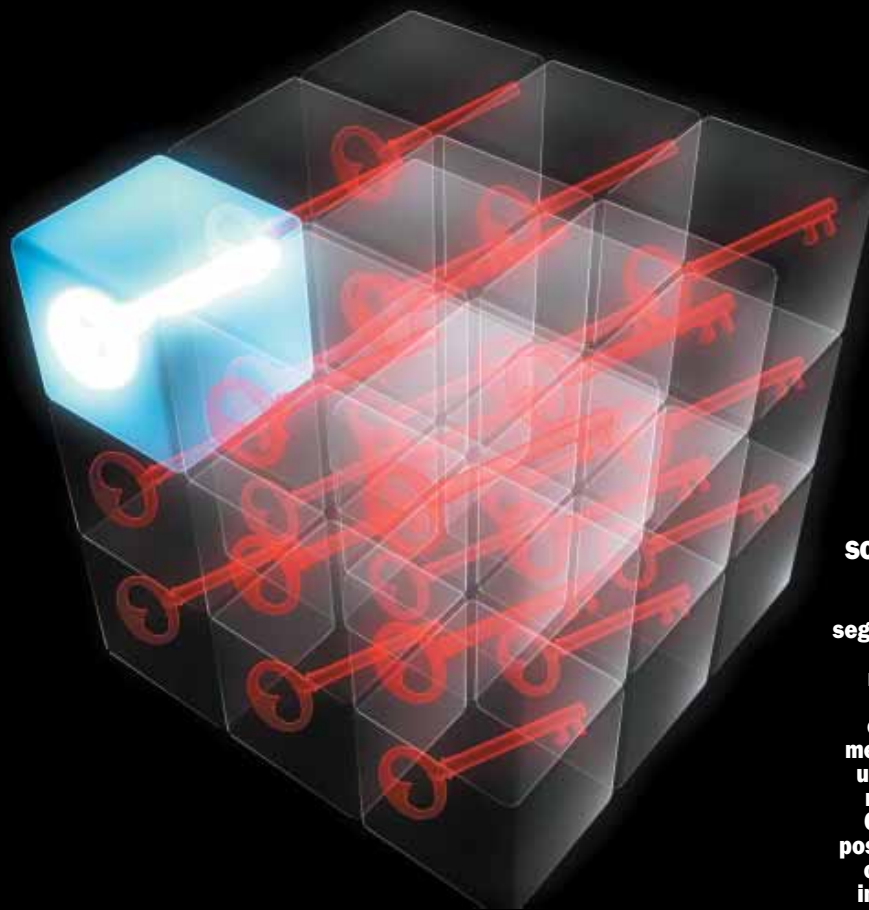
Basterebbero 300 qubit per superare tutti i computer "classici"

Messaggi sotto chiave
Per crittare i messaggi segreti si usano sequenze di numeri dette "chiavi" (da combinare al messaggio con un'operazione matematica). Con i qubit si possono creare chiavi sicure, impossibili da intercettare.

zo di operazioni logiche che, combinate tra loro, danno vita a un "algoritmo" (cioè un insieme di regole per risolvere un problema matematico)» spiega Rosario Fazio, docente di fisica alla Sissa (Scuola internazionale superiore di studi avanzati) di Trieste. «In un computer quantistico, invece, i "qubit" (così si chiamano i "bit quantistici") possono essere anche una "sovrapposizione" di 0 e 1». Un bit quantistico, insomma, può essere 0, 1 o una combinazione dei due: un po' come una moneta che possa essere testa o croce contemporaneamente (la possiamo pensare come inclinata, *v. figura nella prima pagina*). O come una persona con il dono dell'ubiquità, che possa stare in due posti nello stesso tempo. I qubit mantengono questa caratteristica bizzarra finché sono isolati dal mondo esterno e in questo modo possono effettuare tutti i loro calcoli. Ma, secondo le leggi quantistiche, quando si guarda il risultato del calcolo, i qubit si trasformano irrimediabilmente in bit normali.

Come tanti computer

Il primo ad accorgersi che i qubit si potevano usare per costruire, in linea di principio, computer potentissimi fu il fisico e premio Nobel Usa Richard Feynman, nel 1982: grazie ai qubit, capì Feynman, si potevano effettuare calcoli capaci di prendere in esame in un solo momento tutte le possibili combinazioni di 0 e 1.

In pratica, era come avere in un solo computer quantistico tantissimi (anche miliardi) computer tradizionali in parallelo. Restava, però, un problema. «Le operazioni logiche fondamentali servivano per operare sui bit classici e non su quelli quantistici» spiega Fazio. «Erano, insomma, inadatte allo scopo. Bisognava crearne di nuove. Nel 1985, però, il fisico britannico David Deutsch dimostrò come doveva funzionare in concreto un computer quantistico, sulla base di una nuova classe di operazioni logiche». Non solo: Deutsch dimostrò anche che un computer quantistico poteva svolgere tutti i calcoli realizzabili da un computer classico. E, anzi, che era superiore: fece notare che, mentre un computer classico deve effettuare due operazioni per guardare i due lati di una moneta (e decidere se sono uguali o no), un

Connessioni in sicurezza

A lato: laser all'Università di Vienna, dove si studiano sistemi di comunicazione quantistici (ultrasicuri). Sotto, comune bancomat: usa sistemi di sicurezza che un computer quantistico violerebbe facilmente.

3) Il sogno di tutte le spie

Un computer quantistico è molto più veloce di un computer classico a suddividere un numero in un prodotto di altri numeri "primi" (cioè non più scomponibili nello stesso modo). Questa operazione è utile per trovare la "chiave" per decrittare i messaggi top secret.

Scusi, dov'è...
Biblioteca antica del Trinity College di Dublino, in Irlanda. Per cercare un libro nei suoi archivi, un computer classico dovrebbe esaminarli tutti uno a uno. Un computer quantistico, invece, sarebbe più veloce.

Il primo prototipo fu costruito nel 2001. E calcolò 15 = 3x5

computer quantistico può farlo in un colpo solo.

Potenziale scassinatore

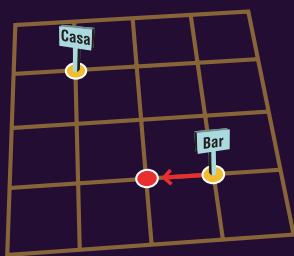
La superiorità di un computer quantistico per operazioni di interesse pratico, però, fu dimostrata solo nel 1994, dal fisico Peter Shor. «Shor trovò un algoritmo efficace per scomporre qualsiasi numero intero nel prodotto di numeri primi (cioè numeri interi non ulteriormente scomponibili)» dice Fazio. Che interesse può avere una simile operazione? Può servire ad esempio a trovare la "chiave" per rendere leggibile a un intruso le comunicazioni in codice che usiamo inconsapevolmente quando paghiamo con il bancomat o facciamo un acquisto su Internet. La chiave, infatti, è un numero primo con molte cifre che viene "combinato" (con un processo matematico) a un messaggio (che può essere anche una transazione monetaria) per renderlo incomprensibile agli intrusi.

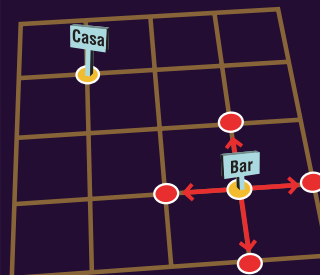
Fin qui è solo teoria. I computer quantistici funzionanti, però, ci sono già. Il primo è stato costruito nel 2001 da Isaac Chuang, presso il centro di ricerca Ibm di Almaden, in California (Usa). Consisteva in una molecola artificiale in cui erano "immagazzinati" 5 qubit. L'informazione si poteva acquisire e leggere grazie alla risonanza magnetica, un fenomeno (basato sul magnetismo molecolare) usato anche a scopo diagnostico negli ospedali. Con il suo apparato di misura, Chuang è riuscito a effettuare un semplice calcolo: ha scomposto il numero 15 nel prodotto di due numeri primi, 3 e 5 (15=3x5). È un'operazione semplice, ma concettualmente si può estendere fino a numeri giganteschi. Il problema è creare e manipolare una quantità maggiore di qubit.

Atomi artificiali

«Le tecniche basate sulla risonanza magnetica sono quelle che finora hanno dato i risultati migliori» spiega Fazio «ma hanno

Qubit "super"
Rosario Fazio, fisico: studia i computer quantistici con circuiti super conduttori.

4) Così rincasa un ubriaco "classico"...

Un ubriaco "classico" esce dal bar e deve tornare a casa. Non si ricorda nulla e vive in un paese squadrato, composto da 5 vie che incrociano altre 5 vie. Come fa? Sceglie una direzione a caso, va avanti fino al primo incrocio. Poi ricomincia: sceglie una strada a caso, va avanti fino al primo incrocio. E così via, fino a quando, dopo 25 tentativi in media, arriva a casa.

... e così un ubriaco "quantistico"

Un ubriaco "quantistico", invece, esce dal bar e può percorrere contemporaneamente tutte e 4 le direzioni possibili. Arriva ai 4 incroci e ripete l'operazione: ci mette molto meno tempo (5 tentativi in media) ad arrivare a casa. Operazioni di questo tipo hanno anche applicazioni pratiche, per esempio, nel campo dell'economia.

5) Oltre il nostro universo

Secondo David Deutsch, fisico all’Università di Oxford (Uk), le proprietà bizzarre dei computer quantistici si spiegano così: esistono tanti universi paralleli al nostro e ogni qubit si trova contemporaneamente in due universi (in uno vale 1 e nell’altro vale 0). Se i qubit sono due, tutte le possibili combinazioni (00, 11, 01 e 10) si trovano in 4 universi. E così via. Ogni computer quantistico in azione, insomma, equivale a tanti computer classici che effettuano i loro calcoli in parallelo, ciascuno in un universo differente.

Mondi paralleli.

Un computer quantistico permetterebbe di violare gli attuali codici top secret

un inconveniente: non si sa come renderle più complesse». Per manipolare più qubit, infatti, servirebbero molecole più grandi, ma attualmente nessuno le saprebbe produrre.

«Esistono, però, anche altre tecniche per costruire computer quantistici» continua Fazio «per esempio si possono usare atomi freddi (cioè a temperature prossime allo zero assoluto, pari a -273,15 °C), come si sta sperimentando all’Università di Innsbruck (Austria) o al Nist (National institute of standards and technology) negli Usa. Oppure si potrebbero usare dispositivi “a stato solido”, basati su materiali superconduttori o semiconduttori». Questi ultimi sono forse i più promettenti, perché l’attuale tecnologia è in grado di manipolarli meglio. Si tratterebbe, infatti, di un’evoluzione dei circuiti di silicio che esistono già. I circuiti superconduttori (*v. foto a lato*) contengono materiali che conducono l’elettricità senza dissipare energia. Quelli a semiconduttore, invece, contengono strutture simili ad atomi artificiali: a differenza degli atomi reali, possono essere costruiti “su misura” nelle dimensioni e nelle quantità volute. Ma hanno pure svantaggi: a differenza degli atomi reali, non sono tutti uguali tra loro.

Qubit in un circuito superconduttore.

In arrivo nel 2008

E allora, quando avremo il primo computer quantistico in grado di effettuare operazioni complesse? La società canadese D-wave ha annunciato che costruirà il primo prodotto commerciale nel 2008. Non si sa ancora di che cosa si tratti. Ma probabilmente, se sarà davvero costruito, sarà un singolo dispositivo, di cui la società venderà il “tempo macchina”, capace di svolgere calcoli specialistici da integrare poi con i computer normali.

In una direzione simile, comunque, punta anche l’Unione europea. «Uno dei progetti di ricerca finanziati dall’Ue» dice Fazio «riguarda le applicazioni con pochi qubit: si punta a sistemi di una ventina di qubit, quel che basta a compiere calcoli di una certa complessità». Se poi si riuscisse a costruire un computer di “soli” 300 qubit, in linea di principio si avrebbe più potenza di calcolo di un computer classico con tanti bit quante sono tutte le particelle dell’universo! Peccato che un computer del genere non potrebbe sfruttare appieno la sua potenza... I computer quantistici, infatti, sono ben più “delicati” di quelli tradizionali, perché i qubit tendono a trasformarsi, a caso, in bit semplici (0 o 1). Per questo motivo, un buon computer quantistico deve spendere il 99% circa del suo tempo a correggersi.

Esiste già?

E allora, tutto è pronto per questa nuova rivoluzione tecnologica. I primi computer quantistici complessi potrebbero esistere già, nascosti ad esempio nelle stanze del Pentagono. Tecnicamente è possibile. E certamente questa tecnologia fa gola ai servizi segreti. Si stima, infatti, che occorrerebbero molti miliardi di anni (più dell’età dell’universo) affinché tutti i computer esistenti possano decrittare un messaggio con una chiave di 1024 bit, lo standard attuale per le comunicazioni top secret. Un computer quantistico, invece, ci metterebbe pochi giorni. ■

Andrea Parlangeli

Per saperne di più:
Su Internet: *http://cordis.europa.eu/ist/fet/qipc-eu.htm.* Sito dell’Ue dedicato alla ricerca sui computer quantistici (in inglese).

7) Teletrasporto (di qubit)

Nel mondo quantistico, esiste il fenomeno del teletrasporto (v. Focus n° 104): le proprietà delle particelle possono essere cioè trasferite da un posto a un altro in maniera rapidissima, talvolta anche istantaneamente. Questo fenomeno si può usare nei computer quantistici, per spostare l’informazione di un qubit da un punto a un altro del circuito.

Molecola calcolatrice
Steffen Glaser, chimico all’Università di Monaco, in Germania, mostra il modello di una molecola usata come computer.

6) Le comunicazioni del futuro

Sfruttando le proprietà quantistiche, è possibile inviare messaggi crittati in maniera perfettamente sicura (cosa che non si può fare con un sistema classico). A causa della “delicatezza” dei qubit, infatti, un sistema quantistico si accorgerebbe se qualcuno cercasse di intromettersi nella comunicazione e modificherebbe la parola chiave. In questo caso non si tratta di computer, ma di sistemi di comunicazione, basati per esempio sulle fibre ottiche. Esistono già alcuni prototipi. Come “Vectis”, prodotto dell’azienda svizzera Id Quantique: funziona fino a 100 km di distanza e costa 100 mila €.